MPD 2810.1
REVISION A
EFFECTIVE DATE: June 11, 2003
EXPIRATION DATE: June 11, 2008

# MARSHALL POLICY DIRECTIVE

## AD01

# SECURITY OF INFORMATION TECHNOLOGY

## DOCUMENT HISTORY LOG

| Status (Baseline/ Revision/ Canceled) | Document Revision | Effective Date | Description |
|---|---|---|---|
| Baseline | | 11/22/99 | |
| Revision | A | 6/11/2003 | Section 7.6, fourth line, added “processes described in”; sections 7.11 and 8.3, added “Office of the”; changed heading title in section 8.3; changed “IT Resource” to “System and Network” in section 8.7 heading; and added “IT System” to heading in section 8.8. |
| | | | |
| | | | |

## 1. PURPOSE

The purpose of this Directive is to ensure the implementation of a MSFC Information Technology (IT) security program that meets minimum Federal and Agency requirements and adequately protects the MSFC IT investment, while supporting the enterprise, program, and project activities of the Center. These policies are consistent with NASA Policy Directive (NPD) 2810.1, and NASA Procedures and Guidelines (NPG) 2810.1, "Security of Information Technology," to require that all information stored, transmitted, or processed within NASA networks be safeguarded consistent with the level of risk and potential for impact to Agency missions that may result from loss, alteration, unavailability, or misuse of the information.

## 2. APPLICABILITY

This Marshall Policy Directive (MPD) applies to all employees, MSFC contractor employees, to the extent of the in-force contract or grant, in achieving MSFC missions, programs, projects, and institutional requirements. The directive addresses all MSFC IT resources, including all networks, systems, services; applications connected to the MSFC IT network infrastructure; and all MSFC IT resources outsourced to: (1) another Center; (2) another Government Agency; or (3) a commercial facility.

## 3. AUTHORITY

This policy directive is maintained by the MSFC Office of the Chief Information Officer (CIO) and is authorized by NPD 2810.1, "Security of Information Technology."

## 4. APPLICABLE DOCUMENTS

a. Office of Management and Budget (OMB) Circular A-130, "Management of Information Technology Resources"

b. NPD 2810.1, "Security of Information Technology"

c. NPG 2810.1, "Security of Information Technology"

d. MPG 2810.1, "Security of Information Technology"

e. MPG 1410.2, "Marshall Management Directives System"

## 5. REFERENCES

None

## 6. DEFINITIONS

a. Compromised Resource. An IT resource for which access to system ("root") level privileges or rights is gained by an unauthorized user.

b. IT Resource. A computer workstation, data or application server, network connectivity or protective equipment, or other data-processing element that provides an IT system, application, or service function.

c. IT Security Team. A group of representatives of MSFC organizations, including contractor IT service providers and outsourcers, to coordinate IT security program planning and implementation.

d. Line Manager. A civil service department manager or group lead who exercises administrative or operational controls, whether directly or through delegated technical civil service or contractor staff, for an IT resource in his/her area of responsibility.

e. MSFC IT Security Infrastructure. The network of data processing elements including firewalls, data routers and switches, hubs, and gateways that interconnect MSFC IT resources to provide Centerwide security features against external threats and intrusions.

f. Software Patch. A set of software codes or routines that forms an update or "fix" to an operating system, application, or data file.

g. Stand-alone Resource. An IT resource that is not connected to a data network.

## 7. POLICY

This Directive is in concert with the requirements of NPD 2810.1, "Security of Information Technology," to ensure adequate security is provided for all MSFC information which is collected, processed, transmitted, stored, or disseminated.

MSFC IT security resources shall be acquired, used, and retired in a manner which (1) includes and integrates high-performance

security architectures; (2) maximizes integrated architectures and standards; (3) contributes to open, standardized, scaleable, interoperable, and yet secure IT environments, to the extent practicable; (4) meets mission needs; and (5) is cost effective.

7.1 Security Infrastructure

The MSFC IT network security infrastructure shall be planned, developed, installed, and maintained in an integrated, Centerwide configuration that maximizes data performance and operational serviceability, with an emphasis on damage containment and recovery potential capabilities following a security incident.

The IT infrastructure shall comprise host networks implemented with levels of protective isolation and separation between network segments to provide required security features. All MSFC networked IT resources shall be connected to the MSFC IT infrastructure in a manner that accounts for their minimum security needs, the assessment of the value of the information processed by the resource, the assessed risks to that information, and the similarity of security needs and risks to those of other connected resources.

7.2 Stand-alone Resources

Stand-alone IT resources, while not required to meet the security requirements of any particular host network, shall nonetheless meet the minimum-security requirements given in NPG 2810.1.

7.3 Risk Management

The level of security risk to IT investments shall be managed through the conduct of resource vulnerability scanning and risk assessments, and the development of comprehensive security plans for individual resources, considering the major factors in risk management: (1) the value of the resource; (2) the perceived or real threat or threat level; (3) operational vulnerabilities; (4) recovery of operations; and (5) the effectiveness of current or proposed safeguards.

7.4 Life-Cycle Decisions

Life-cycle-based planning, budgeting, and investment control decisions shall be made to mitigate IT risks consistent with advances in IT networking and data processing developments, and sound technical and business judgement, while complying with MSFC planning, capital investment, and program/project management

processes. Funding requirements shall be identified to, and addressed by, in-place and projected funding resources.

7.5 Proper Use

All IT systems and services on any MSFC domain network are Federal resources and shall be used only for authorized purposes. A warning and notification shall be provided on all MSFC IT resources at time of system log-on or challenge for user authentication, advising the user of the potential for system and keystroke monitoring of the user's activity, as well as possible disciplinary action and prosecution arising from unauthorized use of the resource.

7.6 Incident Response and Recovery

Security incidents shall be identified and addressed in a manner appropriate to the criticality of the impacted IT resource and associated data. Compromised resources shall be isolated from the MSFC network infrastructure until remediated per processes described in MPG 2810.1. Following a security incident, a description of the incident, steps taken to stabilize the impacted resource, and measures planned, recommended, or employed to mitigate further incident occurrences, shall be documented for use in methods of continuous improvement of the MSFC IT investment. The estimated cost impact due to a security incident shall be calculated and included in required incident metrics reporting.

7.7 Training

All MSFC employees shall receive adequate training to properly fulfill their IT security responsibilities. All contractor employees shall be informed of these security responsibilities, with appropriate training provided to the extent allowed by the provisions of their contract.

7.8 Access

User access to MSFC IT resources shall be granted in accordance with NPG 2810.1 and shall include the minimum privileges necessary for the resource users to accomplish their assigned tasks. Where required, appropriate personnel screening for users shall be completed prior to granting of access to MSFC IT resources.

7.9 Periodic Review

Network architectures and security infrastructure interconnections shall be periodically reviewed to assure a provision of adequate levels of security.

7.10 Compliance

The planning, acquisition, installation, use, and retirement of MSFC IT architectures, systems, applications, and networks shall comply with applicable Federal, Agency, and MSFC IT policies, guidance, and requirements. It is the responsibility of all MSFC employees and contractors (to the extent provided for by the in-force contract or grant) to comply with this policy and related guidance. Failure to comply may result in isolation of the affected or subject IT resources from the MSFC network infrastructure, and/or adverse administrative personnel or criminal action.

7.11 Waiver

All requests for waiver to this document shall be submitted to the MSFC Office of the CIO for review and consideration before being processed per MPG 1410.2.

7.12 Administration and Management

Those personnel responsible for administration and management of MSFC IT resources shall receive training adequate to the level of their responsibilities, and shall install, configure, operate, and maintain those resources per the requirements of Federal, NASA, and MSFC policy, with special emphasis on the timely installation of software security updates and adequate personnel access controls.

7.13 Passwords

All users and administrators of MSFC IT resources shall implement password creation and usage practices per NPG 2810.1.

7.14 Data Backup

All information processed by MSFC IT resources shall be maintained with data backups adequate to the sensitivity and value of the information involved.

7.15 Retirement and Disposal

All MSFC IT resources shall be retired or disposed of in such a manner so as to protect the confidentiality of the information processed during the use of the resource. Third-party licensed software shall be protected to the extent required by the requirements of the owner's usage license.

## 8. RESPONSIBILITIES

All MSFC employees are responsible for the security of MSFC IT resources. Specifically, the security of individual MSFC IT resources is the ultimate responsibility of the resource owner organization, with specific responsibilities assigned to the cognizant line manager for the resource. Certain MSFC organizations identified in this policy directive shall perform key IT security roles and duties.

8.1 Chief Information Officer (CIO)

The MSFC CIO shall provide management oversight for ensuring the confidentiality, integrity, and availability of all MSFC IT resources.

8.2 IT Security Manager (ITSM)

The MSFC ITSM is responsible for the planning, coordination, and oversight of initiatives and measures to ensure the confidentiality, integrity, and availability of MSFC IT resources and information, consistent with the operational needs of MSFC's missions, programs, and projects.

8.3 Office of the CIO

The MSFC Office of the CIO is responsible for the implementation of all Centerwide MSFC IT security infrastructure services to adequately meet policy and guidelines prescribed by Agency and MSFC directives, and for the integration of security configurations of individual MSFC IT resource owners.

8.4 Employee Organizational and Development Department (EODD)

The MSFC EODD is responsible for implementation of a Centerwide IT security training program, in coordination with the activities of ITSM, to adequately meet Federal, Agency, and MSFC requirements.

8.5 IT Security Team

The IT Security Team is responsible for developing coordinated, Centerwide planning, approaches, and architectures for a MSFC IT security program that is adequate to ensure the confidentiality, integrity, and availability of MSFC IT resources and information.

8.6 Organizational Computer Security Official (CSO)

MSFC Organizational CSOs are responsible for the coordination of IT security for computer resources or services residing in, or served from, that organization. This includes the establishment of management controls and communication processes to the organization's personnel to ensure that implementation of IT security requirements is consistent with MSFC mission needs, policy, and guidance.

8.7 System and Network Administrator

System and Network Administrators of MSFC IT resources shall install, configure, operate, and maintain those resources in their areas of control per all applicable Federal, NASA, and MSFC IT security policies and guidance.

8.8 IT System Line Manager

A civil service line manager who is functionally associated with an IT resource shall be responsible for ensuring the resource performs as designed and meets the needs of customers and data owners. If the resource is operated by a MSFC contractor, this responsibility shall be assigned to the cognizant civil service manager for the resource or contract.

## 9. RECORDS

None

## 10. MEASUREMENTS

Measurements shall be collected and evaluated at least annually to assess the effectiveness of this policy by measuring the degree of compliance with assignments of responsibility for IT security, the establishment of security plans, the review of security controls, and the documented authorizations that security plans are adequately implemented.

## 11. CANCELLATION

MPD 2810.1 dated November 22, 1999

Original signed by
Axel Roth for

A. G. Stephenson
Director